

In re: David M. Blaker
Serial No.: 10/004,081
Filed: October 30, 2001
Page 13

REMARKS

Applicant appreciates the Examiner's thorough examination of the present application as evidenced by the Office Action of July 1, 2005 (hereinafter "Office Action"). Applicant especially appreciates the indication that Claims 4, 5, 8, 9, 19, 20, 23, 24, 28, 29, 32, and 33 recite patentable subject matter. In response, Applicant has amended independent Claims 1, 16, and 25 to clarify that the sequential random values are determined for the stream cipher. Applicant has also amended various other claims to address Sec. 112 rejections. Applicant respectfully submits that the cited reference fails to disclose or suggest, among other things, all of the recitations of independent Claims 1, 16, and 25. Accordingly, Applicant submits that all pending claims are in condition for allowance. Favorable reconsideration of all pending claims is respectfully requested for at least the reasons discussed hereafter.

Restriction Requirement

Applicant confirms the election of Claims 1 - 9 and 16 - 33 without prejudice or disclaimer. Applicant agrees that the unpatentability of Claims 10 - 15 would not necessarily imply the unpatentability of Claims 1 - 9 and 16 - 33.

Information Disclosure Statement

The Schneier reference submitted as part of an Information Disclosure Statement on January 9, 2003 has not been considered by the Examiner. Applicant submits herewith the Schneier reference along with a page identifying the copyright date of the Schneier reference.

Claim Objections

Independent Claims 1, 16, and 25 stand objected to because they recite "an stream cipher." In response, Applicant has amended this recitation to be "a stream cipher."

Section 112 Rejections

Dependent Claims 3 - 5, 7 - 9, 18 - 20, 22 - 24, 27 - 29, and 31 - 33 stand rejected under 35 U.S.C. §112 as being indefinite. In response, Applicant has amended Claims 3, 7, 18, 22, 27, and 31 to clarify that the values of the counters are utilized in determining the at least two sequential random values.

In re: David M. Blaker
Serial No.: 10/004,081
Filed: October 30, 2001
Page 14

Section 101 Rejections

Independent Claims 1 and 25 stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. As discussed in the Manual Of Patent Examining Procedure (MPEP):

The claimed invention as a whole must accomplish a practical application. That is, it must produce a "useful, concrete and tangible result." *State Street*, 149F.3d at 1373, 47 USPQ2d at 1601-02. The purpose of this requirement is to limit patent protection to inventions that possess a certain level of "real world" value, as opposed to subject matter that represents nothing more than an idea or concept, or is simply a starting point for future investigation or research....

[T]he following [example illustrates a] claimed [invention] that [has] a practical application because [it produces] useful, concrete, and tangible result: ...

- "[T]ransformation of data, representing discrete dollar amounts, by a machine through a series of mathematical calculations into a final share price, constitutes a practical application of a mathematical algorithm, formula, or calculation, because it produces 'a useful, concrete and tangible result' -- a final share price momentarily fixed for recording and reporting purposes and even accepted and relied upon by regulatory authorities and in subsequent trades." *State Street*, 149 F3d at 1373, 47 USPQ2d at 1601....

MPEP, Sec. 2106(II)(A.), page 2100-6, cols. 1-2. (Underline added) As further discussed in the MPEP:

Office personnel have the burden to establish a *prima facie* case that the claimed invention as a whole is directed to solely an abstract idea or to manipulation of abstract ideas or does not produce a useful result. Only when the claim is devoid of any limitation to a practical application in the technology arts should it be rejected under 35 U.S.C. Sec. 101. ...

An applicant may assert more than one practical application, but only one is necessary to satisfy the utility requirement.

MPEP, Sec. 2106(II)(A.), page 2100-7, col. 1. (Underline added.)

Claims 1 and 25 have been amended to indicate that the at least two sequential random values are determined for the stream cipher. As is well known to those of skill in the art of cryptography, a stream cipher is a symmetric cipher in which plaintext digits are encrypted one at a time, and in which the transformation of successive digits varies during the encryption. Applicant respectfully submits that a stream cipher is a useful, concrete, and tangible result in the field of cryptography. In addition, Applicants submit that Claims 1 and 25 are not devoid of any limitation to a practical application in the technology arts as set forth

In re: David M. Blaker
Serial No.: 10/004,081
Filed: October 30, 2001
Page 15

above.

Accordingly, Applicants respectfully submit that Claims 1 and 25 meet all the requirements of 35 U.S.C. §101.

Section 102 Rejections

Independent Claims 1, 16, and 25 stand rejected under 35 U.S.C. §102(e) as being anticipated by U. S. Patent No. 6,490,354 to Venkatesan et al. (hereinafter "Venkatesan"). (Office Action, page 7). Independent Claims 1, 16, and 25 are directed to a method, system, and computer program product for determining random values for a stream cipher in which at least two sequential random values for the stream cipher are determined in parallel using a common S-box.

Venkatesan describes a keystream generator in which procedure 620 of FIG. 6 is iteratively executed to generate a continuous pseudo-random word sequence. (See, e.g., Venkatesan, col. 10, lines 35 - 41). Thus, in sharp contrast with the recitations of independent Claims 1, 16, and 25, Venkatesan does not describe or suggest determining sequential random values in parallel using a common S-box.

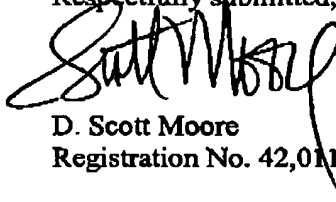
Accordingly, for at least the foregoing reasons, Applicants respectfully submit that independent Claims 1, 16, and 25 are patentable over Venkatesan, and that Claims 2 - 9, 17 - 24, and 26 - 33 are patentable at least as they depend from an allowable claim.

In re: David M. Blaker
Serial No.: 10/004,081
Filed: October 30, 2001
Page 16

CONCLUSION

In light of the above remarks, Applicant respectfully submits that the above-entitled application is now in condition for allowance. Favorable reconsideration of this application is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

Respectfully submitted,

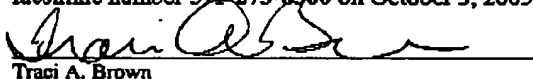


D. Scott Moore
Registration No. 42,011

Myers Bigel Sibley & Sajovec, P.A.
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401
Customer Number 20792

CERTIFICATION OF FACSIMILE TRANSMISSION UNDER 37 CFR 1.8

I hereby certify that this correspondence is being facsimile transmitted to the Patent and Trademark Office via facsimile number 571-273-8300 on October 3, 2005.



Traci A. Brown